LIS565 Lecture 6

Thomas Krichel

http://openlib.org/home/krichel

2001–11–08

Reading

Comer chapter 12, 13, 20, 21, 23

Structure

Network Address Translation (NAT)

User Datagram Protocol (UDP)

Dynamic Host Configuration Protocol

Transmission Control Protocol

Network Address Translation (NAT)

Allows hosts on a private network to access sites on the Internet.

The private network runs IP protocols, but with private addresses

- 10.???.???.??? (class A)
- 192.???.???.??? (class B)

A gateway machine translates requests from the internal machine IP addresses to its external addresses.

There are various ways of doing this.

User Datagram Protocol

In IP, packets are sent to a host. Where on the host should the data go to?

Usually the host can do many things, i.e. it has multitasking capability. A software that is running on a computer is called a process.

UDP provides a way to send unreliable packets to specific process.

talking to processes

Internet protocols do not communicate with application processes

- processes could start end at any time
- software may be updated and require a different way to talk to

therefore Internet packets arrive at ports

port

a port is identified by a positive integer number.

processes check ports for data that has arrived.

if data arrives while the process is not listening, data is stored at the port.

Example: web server sends pages and listens to now requests.

User Datagram Protocol

UDP provides an unreliable connectionless delivery service using IP to transport messages between hosts. It uses IP but adds the ability to distinguish among multiple ports.

UDP

Two word header. Word one:

Source port (16 bits)
Destination port (16 bits)

Word 2:

UDP message length in bytes (16 bits)
UDP checksum (16 bits)

The checksum covers the IP destination address as well. The IP destination address is in the IP header, of course.

After that comes the data.

Well-known ports

Two ways to assign ports to processes.

One is central authority: everybody uses the same "well-known" port. All ports < 1024 are well-known ports.

example:

http uses port 80

telnet uses port 25

bind uses port 53

application: usage of ports in NAT

NAT, among other methods, can use port numbers. It assigns a different source port for each outgoing communication that a machine wishes to make on the Internet.

When the response comes off the Internet, the NAT server translates the port back to a private IP number and its port.

application: firewall

A firewall is a device that can filter traffic following rules about

- source IP address
- destination IP address
- destination port
- source port

and others.

application: DHCP

DHCP is the dynamic host configuration protocol. It is an alternative to RATP.

Using DHCP, a host uses UDP to discover its IP address.

This may appear strange.

leasing an IP address

client—that does not have an IP address—sends DHCPDISCOVER message.

It is a broadcast message. The port is 67, the well-known port for DHCP.

One or more DHCP severs send a DHCPOFFER.

The client picks one of the servers that issued the DHCPOFFER and sends a DHCPREQUEST. The server answers with the DHCPACK that contains the address.

The address is leased, i.e. only valid for a certain time.

reliable communication

UDP is an unreliable transport layer.

TCP is an reliable transport layer.

Reliable means

- stream orientation. bytes come out from the sender, arrive in the same order at the receiver
- virtual circuit connection: the sequence of IP appears like a connection
- buffering: fast arrived data is stored at the destination until it can be processed
- full duplex: communication in two ways.

positive acknowledgement with retransmission

is the idea behind (almost all) reliable communication. In its simplest form.

Sender send packet 1.
Receiver sends acknowledgment message for packet 1

Sender send packet 2
Receiver sends acknowledgment message for packet 2

- each machine waits. verrry slow.
- delayed duplicates can cause all sorts of problems

sliding window protocol

Generalization of the previous idea. Example with window size 3.

Sender sends P1, P2, P3, waits. When acknowledgement A1 arrives, sends P4.
When acknowledgement A2 arrives, and P4 has been sent, sends P5.

Transmission Control Protocol (TCP)

TCP specifies the format of the data and acknowledgments that two computers exchange to achieve a reliable transfer.

TCP transports data between endpoints. Endpoints are pairs (IP number, port).

It uses sliding window protocol with varying window size over time.

TCP segment

has a header and a body.

Header has at least 3 words. Word 1

Source port (16 bits)
Destination port (16 bits)

Word 2:

number of this segment

Word 3:

next segment expected

Word 4:

other stuff

Word three has the number of a segment from the other host that the sending host is waiting for.